ELSEVIER

Discrete Mathematics 208/209 (1999) 139–156

DISCRETE MATHEMATICS

Cyclic and elementary abelian caps in projective spaces

A. Cossidente[a], L. Storme[b,*]

[a] *Dipartimento di Matematica, Università della Basilicata, Via N. Sauro 85, I-85100 Potenza, Italy*
[b] *Department of Pure Mathematics and Computer Algebra, University of Gent, Galglaan 2, 9000 Gent, Belgium*

Received 5 March 1997; revised 7 April 1998; accepted 27 April 1998

Dedicated to the memory of G. Tallini

Abstract

This article presents cyclic and elementary abelian caps in projective spaces. Different classes of groups all yielding an infinite class of caps are presented. The link with pseudo-cyclic codes is discussed, and we show that a result by Boros and Szőnyi in $\mathrm{PG}(2,q^2)$ can be extended to $\mathrm{PG}(2n,q^2)$ for proving that the $(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n,q^2)$ constructed by Ebert and Kestenband are equivalent. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Caps; Cap-codes; Groups; Projective spaces

1. Introduction

Let $\mathrm{PG}(N,q)$ be the projective space of dimension N over the finite field $\mathbb{F}_q$ of order q.

An *n-cap* K in $\mathrm{PG}(N,q)$ is a set of n points, no three of which are collinear. An *n-cap* of $\mathrm{PG}(2,q)$ is also called an n-arc [9, p. 285], and an n-cap of $\mathrm{PG}(N,q)$ is called *complete* if it is not contained in an $(n+1)$-cap of $\mathrm{PG}(N,q)$.

The maximum value of n for which there exists an n-cap in $\mathrm{PG}(N,q)$ is denoted by $m_2(N,q)$ [9, p. 285]. This number $m_2(N,q)$ is only known, for arbitrary q, when $N \in \{2,3\}$. Namely, $m_2(2,q) = q+1$ if q is odd, $m_2(2,q) = q+2$ if q is even, and $m_2(3,q) = q^2+1, q > 2$.

With respect to the other values of $m_2(N,q)$, apart from $m_2(n,2) = 2^n$, $m_2(4,3) = 20$, $m_2(5,3) = 56$ [9, p. 285] and $m_2(4,4) = 41$ [5], only upper bounds are known.

Finding the exact value for $m_2(N,q), N \geqslant 4$, and constructing an $m_2(N,q)$-cap is a very hard problem. Different methods have been used to find examples of caps. Some

* Corresponding author. Research Associate of the Fund for Scientific Research Flanders (Belgium).
E-mail addresses: ca015sci@unibas.it (A. Cossidente), ls@cage.rug.ac.be (L. Storme)

PII: S0012-365X(99)00069-2

authors looked at caps contained in quadrics or Hermitian varieties. Other people used cyclic groups having caps as orbits. Also a coding-theoretic approach has been used.

In [4], Ebert constructed cyclic (q^n+1)-caps in $\mathrm{PG}(2n-1,q)$, n even, and cyclic $(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n,q^2)$. In [2], Cossidente and Storme proved that these (q^n+1)-caps are the intersection of $n-1$ linearly independent elliptic quadrics $E_{2n-1,q}$ and that these $(q^{2n+1}+1)/(q+1)$-caps are the intersection of $2n$ linearly independent Hermitian varieties.

The question arises whether cyclic caps exist contained in the intersection of parabolic quadrics or hyperbolic quadrics, or in the intersection of Hermitian varieties in $\mathrm{PG}(2n-1,q^2)$. A first answer was given in [3] where cyclic $(q^n\pm 1)$-caps in the intersection of parabolic quadrics were constructed.

This article presents two classes of cyclic caps in the intersection of elliptic quadrics, and one class of cyclic caps in the intersection of hyperbolic quadrics; solving in this way the presented problem for the quadrics.

We also present three classes of caps which are contained in quadrics and which are orbits of elementary abelian groups.

In a separate section, we discuss the relation of the cyclic $(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n,q^2)$ by Ebert [4] to the $(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n,q^2)$ by Kestenband [12]. Until now, the equivalence of the two constructions was only proved for $n=1$ by Boros and Szőnyi [1]. We show that, by using a recent result on self-dual normal bases, their proof can be generalized to arbitrary n, thereby showing the equivalence of the constructions by Ebert and Kestenband.

2. Cyclic caps and pseudo-cyclic codes

A *linear* $[n,k,d]$ *code* C over $\mathbb{F}_q$ is a k-dimensional subspace of the n-dimensional vector space $V(n,q)$. The *minimum distance* d of the code is the smallest number of positions in which two different elements of C differ. Equivalently, d is the smallest number of non-zero symbols in any non-zero vector of C.

A *generator matrix* G of a linear $[n,k,d]$ code C is a $k\times n$ matrix whose rows form a basis of C.

For $u=(u_1,\ldots,u_n)$ and $v=(v_1,\ldots,v_n)$, let $u\cdot v=\sum_{i=1}^{n}u_iv_i$ be the standard scalar product of u and v. The *dual code* $C^{\perp}$ of an $[n,k,d]$ code C is $C^{\perp}=\{v\in V(n,q)\|\ v\cdot u=0,\forall u\in C\}$. This is an $[n,n-k,d']$ code and an $(n-k)\times n$ generator matrix H of $C^{\perp}$ is called a *parity check matrix* of C.

The fundamental theorem of coding theory states that d is the minimum distance of a linear $[n,k]$ code C if and only if every $d-1$ columns in a parity check matrix H of C are linearly independent, but some d columns are linearly dependent.

As the columns $\{h_1,\ldots,h_n\}$ of a parity check matrix $H=(h_1\cdots h_n)$ of a linear $[n,k]$ code C define n points of $\mathrm{PG}(n-k-1,q)$, this implies that if $d\geqslant 4$, then no three of $h_1,\ldots,h_n$ are linearly dependent. Hence they constitute an n-cap in $\mathrm{PG}(n-k-1,q)$.

This offers a link between $[n,k,d\geqslant 4]$ codes and n-caps in $\mathrm{PG}(n-k-1,q)$.

Let α be a fixed non-zero element of $\mathbb{F}_q$. A code C is called α-*cyclic* if $(x_1,\dots,x_n)\in C$ implies $(\alpha x_n, x_1,\dots,x_{n-1})\in C$. A code is called *pseudo-cyclic* (or *semi-cyclic*) if C is α-cyclic for some $\alpha\in\mathbb{F}_q\backslash\{0\}=\mathbb{F}_q^*$. The 1-cyclic codes are simply called *cyclic codes*.

To describe these pseudo-cyclic codes C, associate the vector $c=(c_0,\dots,c_{n-1})\in C$ with the polynomial $c(X)=\sum_{i=0}^{n-1} c_iX^i$. This leads to the following characterization of these pseudo-cyclic codes.

Theorem 1 (Maruta [14]). *An α-cyclic $[n,k,d]$ code C corresponds to a non-zero ideal of $\mathbb{F}_q[X]/(X^n-\alpha)$. That is, there exists a unique monic polynomial $g(X)$ of minimal degree in C satisfying*:

(1) *$C=\langle g(X)\rangle$, that is, $g(X)$ is the generator polynomial of C*;

(2) *$g(X)$ is a factor of $X^n-\alpha$*;

(3) *Any $c(X)\in C$ can be written uniquely as $c(X)=f(X)g(X)$ in $\mathbb{F}_q[X]$, where $f(X)\in\mathbb{F}_q[X]$ has degree smaller than k. The degree of $g(X)$ is equal to $n-k$*;

(4) *The dual code of C is α^{-1}-cyclic. Moreover $C^{\perp}=\langle X^k h(1/X)\rangle$ with $X^n-\alpha=g(X)h(X)$.*

Theorem 2 (Maruta [14]). (1) *Let C be an $[n,n-k,d]$-code over $\mathbb{F}_q$. Then C is α-cyclic if and only if C has a parity check matrix $[P^{\mathrm{t}},(PT)^{\mathrm{t}},\dots,(PT^{n-1})^{\mathrm{t}}]$, with $P\in\mathbb{F}_q^k\backslash\{(0,\dots,0)\}$ and $T\in\mathrm{GL}(k,q)$ such that $PT^n=\alpha P$, where P^{t} is the transpose of P.*

(2) *Let $g(X)$ be a polynomial of degree k in $\mathbb{F}_q[X]$ dividing $X^n-\alpha$. Then C is an α-cyclic $[n,n-k,d]$ code over $\mathbb{F}_q$ with generator polynomial $g(X)$ if and only if C is a code with parity check matrix $[P^{\mathrm{t}},(PT)^{\mathrm{t}},\dots,(PT^{n-1})^{\mathrm{t}}]$, where $P=(1,0,\dots,0)$ and where T is the companion matrix of $g(X)$, that is,*

$$T=\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \dots & \ddots & \ddots & \ddots & \dots\\ 0 & 0 & 0 & 0 & \cdots & 0 & 1\\ -a_0 & -a_1 & -a_2 & -a_3 & \cdots & \cdots & -a_{k-1}\end{pmatrix},$$

with $g(X)=\sum_{i=0}^{k} a_iX^i$, and with $a_k=1$. So $(-1)^k g(\lambda)=\det(T-\lambda I_k)$.

3. Cyclic caps on quadrics

In [4], Ebert constructed cyclic (q^n+1)-caps in $\mathrm{PG}(2n-1,q)$, n even. These caps are the orbits of a cyclic subgroup H of order q^n+1 of a cyclic Singer group G of $\mathrm{PG}(2n-1,q)$. In other words, H is a subgroup of a cyclic group G acting transitively on $\mathrm{PG}(2n-1,q)$.

In [2], Cossidente and Storme proved that these caps are the intersection of $n-1$ linearly independent elliptic quadrics of $\mathrm{PG}(2n-1,q)$. Hence, Ebert constructed cyclic caps which are the intersection of quadrics.

This led Cossidente and Storme [3] to the construction of two infinite classes of $(q^n \pm 1)$-caps in $\mathrm{PG}(2n,q)$ which are contained in the intersection of n linearly independent parabolic quadrics.

For this construction, they used a description of $\mathrm{PG}(2n,q)$ inspired by Singer [16]. We briefly repeat these descriptions for the caps constructed by Ebert, and for the caps constructed by Cossidente and Storme.

These ideas will then be used in the next section to construct three new infinite classes of cyclic caps and three new infinite classes of elementary abelian caps. For the cyclic caps, also the generator polynomials of the corresponding pseudo-cyclic codes are given.

3.1. Cyclic caps by Ebert

Represent $\mathrm{PG}(2n-1,q)$ by $\mathbb{F}_{q^{2n}} (\mathrm{mod}\, \mathbb{F}_q)$ [7, p. 77]. This means that the points of $\mathrm{PG}(2n-1,q)$ are the non-zero elements of $\mathbb{F}_{q^{2n}}$. The point of $\mathrm{PG}(2n-1,q)$ represented by $x \in \mathbb{F}_{q^{2n}}^* = \mathbb{F}_{q^{2n}} \backslash \{0\}$ is denoted by (x). Two elements x and y of $\mathbb{F}_{q^{2n}}^*$ define the same point of $\mathrm{PG}(2n-1,q)$ if and only if $x/y \in \mathbb{F}_q$.

The line passing through two points $(x_1),(x_2)$ of $\mathrm{PG}(2n-1,q)$ is the set of points $\{(\lambda_1 x_1 + \lambda_2 x_2) \| (\lambda_1,\lambda_2) \in \mathbb{F}_q^2 \backslash \{(0,0)\}\}$; the plane passing through three non-collinear points $(x_1),(x_2),(x_3)$ is $\{(\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3) \| (\lambda_1,\lambda_2,\lambda_3) \in \mathbb{F}_q^3 \backslash \{(0,0,0)\}\}; \ldots;$ the hyperplane passing through $2n-1$ linearly independent points $(x_1),\ldots,(x_{2n-1})$ is $\{(\lambda_1 x_1 + \cdots + \lambda_{2n-1} x_{2n-1}) \| (\lambda_1,\ldots,\lambda_{2n-1}) \in \mathbb{F}_q^{2n-1} \backslash \{(0,\ldots,0)\}\}$.

By using the following result by Seroussi and Lempel [15], a very useful description of the hyperplanes is obtained. Let $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q : x \mapsto \sum_{i=0}^{m-1} x^{q^i}$ be the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Theorem 3. *The m-dimensional vector space $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ has a trace-orthogonal basis $B = \{b_1,\ldots,b_m\}$ over $\mathbb{F}_q$, that is, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b_i b_j) = 0$ for $i \neq j$.*

The existence of such a trace-orthogonal basis B for $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_q$ implies that two sets $[u_1],[u_2]$, where $u_1,u_2 \in \mathbb{F}_{q^{2n}}^*$ and where $[u] = \{x \in \mathbb{F}_{q^{2n}} \| \mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(u \cdot x) = 0\}$, coincide if and only if $u_1/u_2 \in \mathbb{F}_q^*$. Hence these sets $[u]$, which are linear over $\mathbb{F}_q$, constitute all the hyperplanes of $\mathrm{PG}(2n-1,q)$.

Using this description, the mapping $S : (x) \mapsto (\beta x)$, $x \in \mathbb{F}_{q^{2n}}$, β a primitive element of $\mathbb{F}_{q^{2n}}$, is a Singer-cycle, that is, a transformation acting transitively on $\mathrm{PG}(2n-1,q)$.

Let $\xi = S^{(q^n-1)/(q-1)} : (x) \mapsto (\beta^{(q^n-1)/(q-1)} x)$.

Theorem 4 (Cossidente and Storme [2], Ebert [4]). (i) *An orbit, of size q^n+1, under $\langle \xi \rangle$ is the intersection of $n-1$ linearly independent non-singular elliptic quadrics $Q_{a_1},\ldots,Q_{a_{n-1}}$, $a_1,\ldots,a_{n-1} \in \mathbb{F}_{q^n} \backslash \{0\}$, where $Q_a = \{(x) \in \mathrm{PG}(2n-1,q) \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a x^{q^n+1}) = 0\}$.*

(ii) *An orbit, of size q^n+1, under $\langle \xi \rangle$, is a (q^n+1)-cap of $\mathrm{PG}(2n-1,q)$, n even.*

3.2. Cyclic $(q^n \pm 1)$-caps in $\mathrm{PG}(2n,q)$

Let $\mathrm{PG}(2n,q) \cong \mathbb{F}_{q^{2n}} \times \mathbb{F}_q \pmod{\mathbb{F}_q}$. This means that a point is a 2-tuple $(x,y) \in (\mathbb{F}_{q^{2n}} \times \mathbb{F}_q)\backslash\{(0,0)\}$ and two points $(x_1,y_1),(x_2,y_2)$ coincide if and only if $(x_2,y_2) = \rho(x_1,y_1)$, for some $\rho \in \mathbb{F}_q^*$. By using Theorem 3, the sets $[u,v] = \{(x,y) \in (\mathbb{F}_{q^{2n}} \times \mathbb{F}_q)^* \pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(ux) + vy = 0\}$, $(u,v) \in (\mathbb{F}_{q^{2n}} \times \mathbb{F}_q)\backslash\{(0,0)\}$, constitute all the hyperplanes of $\mathrm{PG}(2n,q)$.

Lemma 5 (Cossidente and Storme [3]). *The set* $Q_{a,b} = \{(x,y) \in (\mathbb{F}_{q^{2n}} \times \mathbb{F}_q) \pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax^{q^n+1}) + by^2 = 0\}, a \in \mathbb{F}_{q^n}, b \in \mathbb{F}_q, (a,b) \neq (0,0)$, *is*:

(1) *a non-singular parabolic quadric of* $\mathrm{PG}(2n,q)$ *when* a,b *are non-zero*;

(2) *a quadratic cone with the point* $(0,1)$ *as vertex, and with a non-singular elliptic quadric in the hyperplane* $Y = 0$ *as base when* $b = 0$;

(3) *the hyperplane* $Y = 0$, *counted with multiplicity two, when* $a = 0$.

Theorem 6 (Cossidente and Storme [3]). *Let* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$ *be n linearly independent quadrics such that not all* b_i *are zero, and such that the quadric* $Q_{0,1}$ *is not linearly dependent on* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$.

Then $\bigcap_{i=1}^n Q_{a_i,b_i}$ *is a cyclic* (q^n+1)*-cap of* $\mathrm{PG}(2n,q)$.

Proof. See [3, Theorems 2.4–2.6]. To describe the cyclic groups acting transitively on $\bigcap_{i=1}^n Q_{a_i,b_i}$, let β be a primitive element of $\mathbb{F}_{q^{2n}}$, and let $\omega = \beta^{(q^{2n}-1)/(q-1)}$.

If q is even, or q and n are odd, defining $S : (x,y) \mapsto (\beta^{2(q^n-1)/(q-1)}x, \omega y)$, and if q is odd, n even, then defining $S : (x,y) \mapsto (\beta^{2(q^n-1)/(q-1)}x, -\omega y)$, gives cyclic groups of order q^n+1 acting transitively on $\bigcap_{i=1}^n Q_{a_i,b_i}$. □

Describe $\mathrm{PG}(2n,q) \cong \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q \pmod{\mathbb{F}_q}$. Then a point is a 3-tuple $(x,y,z) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q)\backslash\{(0,0,0)\}$, and $(x_1,y_1,z_1),(x_2,y_2,z_2)$ define the same projective point if and only if $(x_2,y_2,z_2) = \rho(x_1,y_1,z_1)$, $\rho \in \mathbb{F}_q^*$. By Theorem 3, the hyperplanes of $\mathrm{PG}(2n,q)$ are the sets $[u,v,w] = \{(x,y,z) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q)^* \pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ux + vy) + wz = 0\}$, with $u,v \in \mathbb{F}_{q^n}$, $w \in \mathbb{F}_q$, $(u,v,w) \neq (0,0,0)$, and $[u_1,v_1,w_1] = [u_2,v_2,w_2]$ if and only if $(u_2,v_2,w_2) = \rho(u_1,v_1,w_1)$, $\rho \in \mathbb{F}_q\backslash\{0\} = \mathbb{F}_q^*$.

Lemma 7 (Cossidente and Storme [3]). *In* $\mathrm{PG}(2n,q)$, $Q_{a,b} = \{(x,y,z) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q) \pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(axy) + bz^2 = 0\}$, *with* $a \in \mathbb{F}_{q^n}, b \in \mathbb{F}_q$, $(a,b) \neq (0,0)$, *is*:

(1) *a non-singular parabolic quadric if* $a,b \neq 0$;

(2) *the hyperplane* $Z = 0$ *counted with multiplicity two when* $a = 0$;

(3) *a quadratic cone with vertex* $(0,0,1)$ *and with base a non-singular hyperbolic quadric in* $Z = 0$ *when* $b = 0$.

Theorem 8 (Cossidente and Storme [3]). *Let* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$ *be n linearly independent quadrics so that not all* b_i *are zero, and so that the quadric* $Q_{0,1}$ *is not linearly dependent on* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$.

Then these quadrics intersect in $Z=Y=0$, in $Z=X=0$, and in a cyclic (q^n-1)-cap stabilized by $\langle S\rangle$ with $S:(x,y,z)\mapsto(\lambda x, y/\lambda, z)$, λ a primitive element of $\mathbb{F}_{q^n}$.

3.3. Two more classes including the elliptic quadric-cap

3.3.1. Introduction

Let Q be an elliptic quadric in PG$(3,q)$. Let r_1, r_2 be two distinct points of Q. Then there is a cyclic group G of order q^2-1 fixing r_1, r_2, and acting transitively on $Q\backslash\{r_1,r_2\}$. This group G has the additional property of fixing the polar line L of r_1r_2 with respect to Q. This polar line L is skew to Q; so intersects Q in an elliptic quadric on a line.

To embed this cyclic (q^2-1)-cap into an infinite class of caps, describe PG$(2n+1,q)$ by $(\mathbb{F}_{q^{2n}}\times\mathbb{F}_q\times\mathbb{F}_q)(\mathrm{mod}\,\mathbb{F}_q)$. Hence, a point is a 3-tuple $(x,y,z)\in(\mathbb{F}_{q^{2n}}\times\mathbb{F}_q\times\mathbb{F}_q)^*$. The line $L: X=0$ will be the line containing the two fixed points $r_1=(0,1,0)$ and $r_2=(0,0,1)$. The $(2n-1)$-dimensional polar space of L with respect to the quadrics will be $\Pi: Y=Z=0$. Since we want Π to intersect these quadrics in elliptic quadrics, we assume that Π intersects these quadrics in elliptic quadrics as described in Theorem 4.

The hyperplanes of PG$(2n+1,q)$ are the sets $[u,v,w]=\{(x,y,z)\in(\mathbb{F}_{q^{2n}}\times\mathbb{F}_q\times\mathbb{F}_q)^*(\mathrm{mod}\,\mathbb{F}_q)\,|\,\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(ux)+vy+wz=0\}$, with $u\in\mathbb{F}_{q^{2n}}$, $v,w\in\mathbb{F}_q$, $(u,v,w)\neq(0,0,0)$, and $[u_1,v_1,w_1]=[u_2,v_2,w_2]$ if and only if $(u_2,v_2,w_2)=\rho(u_1,v_1,w_1)$, $\rho\in\mathbb{F}_q^*$.

Lemma 9 (Cossidente and Storme [3]). *The set $Q_{a,b}=\{(x,y,z)\in(\mathbb{F}_{q^{2n}}\times\mathbb{F}_q\times\mathbb{F}_q)(\mathrm{mod}\,\mathbb{F}_q)\,|\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax^{q^n+1})+byz=0\}$, with $a\in\mathbb{F}_{q^n}, b\in\mathbb{F}_q, (a,b)\neq(0,0)$, is:*

(1) *a non-singular elliptic quadric if $a,b\neq 0$;*

(2) *the hyperplanes $Y=0$ and $Z=0$ when $a=0$;*

(3) *a quadratic cone with vertex the line $X=0$ and with base the non-singular elliptic quadric $Q_a=\{(x)\in\mathbb{F}_{q^{2n}}(\mathrm{mod}\,\mathbb{F}_q)\,|\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax^{q^n+1})=0\}$ in $Y=Z=0$ when $b=0$.*

Theorem 10. *Let $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$ be n linearly independent quadrics so that not all b_i are zero, and so that the quadric $Q_{0,1}$ is not linearly dependent on $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$.*

Then these quadrics intersect in a $((q^n+1)(q-1)+2)$-cap consisting of $(0,1,0)$, $(0,0,1)$, and a cyclic $(q^n+1)(q-1)$-cap.

Proof. To prove this, the arguments of [3] can be used. To describe the cyclic group, let ω be a primitive element of $\mathbb{F}_{q^{2n}}$ and let $\xi=\omega^{(q^n-1)/(q-1)}$, $\eta=\xi^{q^n+1}$. The mapping $\alpha:(x,y,z)\mapsto(\xi x,\eta y,z)$ is of order $(q^n+1)(q-1)$, fixes all quadrics $Q_{a,b}$, and the orbits of the points $(x_0,y_0,1)$, $x_0,y_0\neq 0$, all are $(q^n+1)(q-1)$-caps. For assume $(x_0,y_0,1)$, $(x_0\xi^i,y_0\eta^i,1)$, $(x_0\xi^j,y_0\eta^j,1)$ are collinear. By applying the mapping $(x,y,z)\mapsto(x/x_0,y/y_0,z)$, we can assume that $(1,1,1)$, $(\xi^i,\eta^i,1)$, $(\xi^j,\eta^j,1)$ are collinear.

We split up the proof into two parts.

Part 1. If $(1,0,0)$, $(\xi^i,0,0)$, $(\xi^j,0,0)$ define the same point, then $(q^n+1)|i$ because $\xi^{q^n+1}=\eta$ is a primitive element of $\mathbb{F}_q$. Let $i=i'(q^n+1)$, then $(\xi^i,\eta^i,1)=(\xi^{i'(q^n+1)},\eta^{i'(q^n+1)},1)=(\eta^{i'},\eta^{2i'},1)$ since $\eta\in\mathbb{F}_q$. So the points $(1,1,1)$, $(\eta^{i'},\eta^{2i'},1)$, $(\eta^{j'},\eta^{2j'},1)$, $j=j'(q^n+1)$, lie in $\langle(1,0,0),(0,1,0),(0,0,1)\rangle$. In this plane, they are three points of a conic; so they are not collinear.

Part 2. Suppose $(1,0,0)$, $(\xi^i,0,0)$, $(\xi^j,0,0)$ do not define the same point. If n is even, then $\{(\xi^i)\|i=0,\ldots,q^n\}$ defines a cyclic (q^n+1)-cap in $\mathrm{PG}(2n-1,q)$ (Theorem 4). So no three of this set are collinear; so neither the corresponding points $(1,1,1),(\xi^i,\eta^i,1),(\xi^j,\eta^j,1)$ are collinear.

If n is odd, then $\{(\xi^i)\|i=0,\ldots,q^n\}$ defines a union of $(q^n+1)/(q+1)$ lines in $\mathrm{PG}(2n-1,q)$ [2, Theorem 3.8]. If $(1,1,1)$, $(\xi^i,\eta^i,1)$, $(\xi^j,\eta^j,1)$ are collinear, then also $(1),(\xi^i),(\xi^j)$ are collinear; hence $(q^n+1)/(q+1)$ divides i [2, Theorem 3.8]; so $\xi^i,\xi^j\in\mathbb{F}_{q^2}$. Then all points linearly dependent on $(1,1,1)$, $(\xi^i,\eta^i,1)$, $(\xi^j,\eta^j,1)$, $(0,1,0)$, $(0,0,1)$ have coordinates in $\mathbb{F}_{q^2}$. So we can continue the argument in $\mathbb{F}_{q^2}$, assume $n=1$ and assume that we are working in $\mathbb{F}_{q^2}\times\mathbb{F}_q\times\mathbb{F}_q\cong\mathrm{PG}(3,q)$.

In $\mathrm{PG}(3,q)$, $|\langle\alpha\rangle|=q^2-1$ and for $n=1$, $Q_{a,b}$ is an elliptic quadric fixed by a cyclic group of order q^2-1. So the orbit of $(1,1,1)$ is a (q^2-1)-cap contained in an elliptic quadric $Q_{a,b}$. So no three of $(1,1,1)$, $(\xi^i,\eta^i,1)$, $(\xi^j,\eta^j,1)$ can be collinear.

Using arguments similar to the previously used arguments, it is shown that $(0,1,0)$, $(0,0,1)$ extend this cap to a $((q^n+1)(q-1)+2)$-cap.

Using the arguments of [3,12], i linearly independent quadrics Q_{a_j,b_j}, with not all b_j equal to zero and with $Q_{0,1}$ linearly independent on these quadrics, intersect in $(q^{2n+2-i}-2q^{n+1}+q^n+q^{n+2-i}-1)/(q-1)$ points. Hence when $i=n$, these quadrics intersect in $(q^n+1)(q-1)+2$ points.

The points $(0,1,0)$ and $(0,0,1)$ trivially belong to this intersection. There also belongs a point $(x_0,y_0,1)$, with $x_0,y_0\neq 0$, to this intersection. For, suppose a point $(x_0,0,1)$, $(x_0,1,0)$ or $(x_0,0,0)$ belongs to this intersection. Since the quadric $Q_{0,1}$ is linearly independent on the quadrics $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$, the elements $a_1,\ldots,a_n$ must be linearly independent elements of $\mathbb{F}_{q^n}$. Hence, the only value x_0 that can satisfy $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a_i x_0^{q^n+1})=0$, $i=1,\ldots,n$, is $x_0=0$. So, no point $(x_0,1,0)$, $(x_0,0,1)$ or $(x_0,0,0)$, with $x_0\neq 0$, can belong to this intersection.

So, if a point (x_0,y_0,z_0), different from $(0,1,0)$ and from $(0,0,1)$, belongs to the intersection of the quadrics, necessarily $x_0\neq 0$, $y_0\neq 0$ and $z_0\neq 0$. □

3.3.2. The second class

It is also possible to consider the cyclic group discussed in Section 3.3.1 starting from the fixed polar line L skew to Q. The planes through L in $\mathrm{PG}(3,q)$ partition Q into $q-1$ conics, or equivalently ellipses in the corresponding affine planes with L as line at infinity, and in the two points r_1 and r_2.

The (q^2-1)-cap $Q\backslash\{r_1,r_2\}$ will now be embedded into a class of $(q^n-1)(q+1)$-caps in $\mathrm{PG}(2n+1,q)$, n odd, consisting of q^n-1 conics in planes through a fixed line L. For this reason, describe $\mathrm{PG}(2n+1,q)\cong\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_{q^2}\,(\mathrm{mod}\,\mathbb{F}_q)$. Then a point is a 3-tuple $(x,y,z)\in(\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_{q^2})^*$. The hyperplanes are $[u,v,w]=\{(x,y,z)\in(\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times$

$\mathbb{F}_{q^2})^* \pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ux+vy)+\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(wz)=0\}$, with $u,v\in\mathbb{F}_{q^n}$, $w\in\mathbb{F}_{q^2}$, $(u,v,w)\neq(0,0,0)$, and with $[u_1,v_1,w_1]=[u_2,v_2,w_2]$ if and only if $(u_2,v_2,w_2)=\rho(u_1,v_1,w_1)$, $\rho\in\mathbb{F}_q^*$.

The line $L: X=Y=0$ will be the line stabilized by the cyclic group. The $(2n-1)$-dimensional polar space of L with respect to the quadrics will be $\Pi: Z=0$ intersecting the quadrics in hyperbolic quadrics described in Lemma 7(3).

Lemma 11 (Cossidente and Storme [3, Lemma 4.9]). *The set* $Q_{a,b}=\{(x,y,z)\in(\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_{q^2})\pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(axy)+bz^{q+1}=0\}$, *with* $a\in\mathbb{F}_{q^n}$, $b\in\mathbb{F}_q$, $(a,b)\neq(0,0)$, *is*:

(1) *a non-singular elliptic quadric if* $a,b\neq 0$;

(2) *the space* $Z=0$ *when* $a=0$;

(3) *a quadratic cone with vertex the line* $X=Y=0$ *and with base the non-singular hyperbolic quadric* $Q_a=\{(x,y)\in\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\pmod{\mathbb{F}_q} \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(axy)=0\}$ in $Z=0$ *when* $b=0$.

Theorem 12. *For n odd, let* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$ be *n linearly independent quadrics so that not all* b_i *are zero, and so that the quadric* $Q_{0,1}$ *is not linearly dependent on* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$.

Then these quadrics intersect in $X=Z=0$, $Y=Z=0$, *and in a cyclic* $(q^n-1)(q+1)$*-cap if q is even, and in a* $(q^n-1)(q+1)$*-cap which is the union of two disjoint cyclic* $((q^n-1)(q+1)/2)$*-caps if q is odd,* $q>3$.

Proof. To prove this theorem, the arguments of the proof of Theorem 10 can be used.

First of all, j linearly independent quadrics Q_{a_i,b_i}, with not all b_i zero, and with $Q_{0,1}$ not linearly dependent on these quadrics, intersect in $(q^{n+2-j}+1)(q^n-1)/(q-1)$ points.

To describe the cyclic group, let λ be a primitive element of $\mathbb{F}_{q^n}$ and $\eta\in\mathbb{F}_{q^2}$ a primitive $(q+1)$-th root of unity. The mapping $\alpha:(x,y,z)\mapsto(\lambda x,y/\lambda,\eta z)$ is of order $(q^n-1)(q+1)/\gcd(q-1,2)$. The group $\langle\alpha\rangle$ fixes all quadrics $Q_{a,b}$, and the orbits of the points $(x,y,1)$, $x,y\neq 0$, all are caps.

We show that the orbit of $(1,1,1)$ under this group is a $((q^n-1)(q+1)/\gcd(q-1,2))$-cap. Assume that $(1,1,1)$, $(\lambda^i,1/\lambda^i,\eta^i)$, $(\lambda^j,1/\lambda^j,\eta^j)$ are collinear. Then there exist $x,y\in\mathbb{F}_q$ such that $1+\lambda^i x=y\lambda^j$, $1+x/\lambda^i=y/\lambda^j$, and such that $1+x\eta^i=y\eta^j$.

Multiplying the first two equations gives $1+(\lambda^i+1/\lambda^i)x+x^2=y^2$ and this implies $\lambda^i+1/\lambda^i\in\mathbb{F}_q$; so $\lambda^i\in\mathbb{F}_{q^2}$. But since n is odd, necessarily $\lambda^i\in\mathbb{F}_q$.

So $i=i'(q^n-1)/(q-1)$. Now $\eta^{(q^n-1)/(q-1)}=\eta$ since $\eta^{q+1}=1$. Hence with $\lambda^{(q^n-1)/(q-1)}=\xi$, we need to consider the three points $(1,1,1)$, $(\xi^{i'},1/\xi^{i'},\eta^{i'})$, $(\xi^{j'},1/\xi^{j'},\eta^{j'})$, $j=j'(q^n-1)/(q-1)$, and we can do the complete reasoning in $\mathbb{F}_{q^2}$; equivalently $n=1$.

These points all lie on $aXY-aZ^{q+1}=0$ which is an elliptic quadric in $\mathrm{PG}(3,q)$.

So no three of them can be collinear. For q even, it is now clear that the orbit of $(1,1,1)$ is a $(q^n-1)(q+1)$-cap. For q odd, $q>3$, the intersection of the n quadrics is the disjoint union of $X=Z=0$, $Y=Z=0$, and of two cyclic $((q^n-1)(q+1)/2)$-caps. If three points of these two caps would be collinear, then the line passing through these three points would be contained in the intersection. Hence this line would contain at least three points of one of these caps. This is false.

So also for q odd, $q>3$, the intersection contains a $(q^n-1)(q+1)$-cap. □

3.4. Generalizing a cap by Glynn

In [6], Glynn constructed a cyclic $(q^2+1)(q+1)$-cap in $\mathrm{PG}(5,q)$ which is the intersection of two hyperbolic quadrics.

To construct these caps, Glynn started with a cyclic Singer group G in $\mathrm{PG}(3,q)$. Considering an orbit of a line, of size q^3+q^2+q+1, under G, he proved that no three concurrent lines of this orbit can be coplanar. Using the Klein correspondence [8], the q^3+q^2+q+1 Plücker coordinates of the lines in the orbit define q^3+q^2+q+1 points on the Klein quadric H in $\mathrm{PG}(5,q)$, no three of which are collinear. Hence, these constitute a (q^3+q^2+q+1)-cap. This cap has the additional properties of being the intersection of two hyperbolic quadrics, and of being stabilized by a cyclic group fixing one line L external to the Klein quadric, and fixing one elliptic quadric $E_{3,q}$ on H in a 3-dimensional space Π skew to L.

Since, in Lemma 4, the elliptic quadric is embedded into the infinite class of (q^n+1)-caps in $\mathrm{PG}(2n-1,q)$, n even, it is now possible to embed this cap by Glynn into an infinite class of cyclic $(q^n+1)(q+1)$-caps in $\mathrm{PG}(2n+1,q)$, n even, which are the intersection of hyperbolic quadrics.

Let $\mathrm{PG}(2n+1,q)\cong \mathbb{F}_{q^{2n}}\times\mathbb{F}_{q^2}\pmod{\mathbb{F}_q}$. Then a point is a 2-tuple $(x,y)\in(\mathbb{F}_{q^{2n}}\times\mathbb{F}_{q^2})^*$. The line $L:X=0$ will be the line stabilized by the cyclic group. The $(2n-1)$-dimensional polar space of L with respect to the quadrics will be $\Pi: Y=0$ intersecting the quadrics in elliptic quadrics described in Lemma 4. The hyperplanes are $[u,v]=\{(x,y)\in(\mathbb{F}_{q^{2n}}\times\mathbb{F}_{q^2})^*\pmod{\mathbb{F}_q}\,\|\,\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(ux)+\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(vy)=0\}$, with $u\in\mathbb{F}_{q^{2n}}$, $v\in\mathbb{F}_{q^2}$, $(u,v)\neq(0,0)$, and with $[u_1,v_1]=[u_2,v_2]$ if and only if $(u_2,v_2)=\rho(u_1,v_1)$, $\rho\in\mathbb{F}_q^*$.

Lemma 13 (Cossidente and Storme [3, Lemma 4.3]). *The set* $Q_{a,b}=\{(x,y)\in(\mathbb{F}_{q^{2n}}\times\mathbb{F}_{q^2})\pmod{\mathbb{F}_q}\,\|\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax^{q^n+1})+by^{q+1}=0\}$, *with* $a\in\mathbb{F}_{q^n}$, $b\in\mathbb{F}_q$, $(a,b)\neq(0,0)$, *is*:

(1) *a non-singular hyperbolic quadric if* $a,b\neq 0$;

(2) *the space* $Y=0$ *when* $a=0$;

(3) *a quadratic cone with vertex the line* $L:X=0$ *and with base the non-singular elliptic quadric* $Q_a=\{(x)\in\mathbb{F}_{q^{2n}}\pmod{\mathbb{F}_q}\,\|\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax^{q^n+1})=0\}$ *in* $Y=0$ *when* $b=0$.

Theorem 14. *Let* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$ *be n linearly independent quadrics so that not all* b_i *are zero, and so that the quadric* $Q_{0,1}$ *is not linearly dependent on* $Q_{a_1,b_1},\ldots,Q_{a_n,b_n}$.

Then these quadrics intersect in a cyclic $(q^n+1)(q+1)$*-cap if n is even.*

Proof. Let $Q_{a_1,b_1},\dots,Q_{a_i,b_i}$ be i linearly independent hyperbolic quadrics such that $Q_{0,1}$ is not linearly dependent on these quadrics, and such that not all b_i are zero. Then $|\bigcap_{j=1}^{i} Q_{a_j,b_j}| = (q^n+1)\,(q^{n+2-i}-1)/(q-1)$.

Hence, for $i=n$, the intersection consists of $(q^n+1)(q+1)$ points.

The intersection is fixed by $\alpha : (x,y) \mapsto (\beta x, \eta y)$ where $\beta = \omega^{(q^n-1)/(q-1)}$, $\eta = \omega^{(q^{2n}-1)/(q^2-1)}$, with ω a primitive element of $\mathbb{F}_{q^{2n}}$, which is a transformation of order $(q^n+1)(q+1)$ when n is even.

Since the elements $a_1,\dots,a_n$ define a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, for a point (x,y) of $\bigcap_{i=1}^{n} Q_{a_i,b_i}$, necessarily $y \neq 0$ [2, Theorem 3.6]. Also $x \neq 0$ since not all b_i are zero.

For n even, the orbit of a point (x,y), $x,y \neq 0$, always is a cyclic $(q^n+1)(q+1)$-cap. For assume that the points $(1,1),(\beta^i,\eta^i)$, (β^j,η^j) are collinear. Since n is even, the set $\{(\beta^i) \| i=0,\dots,q^n\}$ defines a cyclic (q^n+1)-cap in $\mathrm{PG}(2n-1,q)$ (Theorem 4), and so necessarily $i = i'(q^n+1)$, $j = j'(q^n+1)$.

This means that the points are $(1,1)$, $(\eta^{i'(q+1)},\eta^{i'(q^n+1)}) \equiv (1,\eta^{i'(q^n-q)})$ and $(\eta^{j'(q+1)},\eta^{j'(q^n+1)}) \equiv (1,\eta^{j'(q^n-q)})$.

Now $\eta^{i'(q^n-q)} = \eta^{i'q(q-1)}$. For η a primitive element of $\mathbb{F}_{q^2}$, the elements $X = \eta^{i'q(q-1)}$ satisfy $X^{q+1}=1$ and this defines an ellipse in the affine plane $\mathrm{AG}(2,q) \cong \mathbb{F}_{q^2}$. So no three points of the orbit of $(1,1)$ can be collinear. □

4. Caps by Ebert and Kestenband in PG($2n, q^2$)

4.1. Introduction

In Section 3, different classes of cyclic caps which are the intersection of quadrics were discussed. Also, an infinite class of caps, intersections of Hermitian varieties, is known.

In 1980, Kestenband [12] constructed $(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n,q^2)$ which are the intersection of Hermitian varieties. Five years later, Ebert [4] constructed cyclic $(q^{2n+1}+1)/(q+1)$-caps which are the orbits of subgroups of cyclic Singer groups in $\mathrm{PG}(2n,q^2)$.

In 1986, Boros and Szőnyi [1] proved that for $n=1$, the two constructions yield the same caps, while in 1995, Cossidente and Storme [2] proved that the caps by Ebert are the intersection of Hermitian varieties. Hence, the caps by Ebert are of Kestenband-type.

By using a result on self-dual normal bases [11,13], the final link is presented. The caps by Kestenband are orbits of subgroups of cyclic Singer groups. To prove this, we follow the arguments by Boros and Szőnyi [1]. The main problem is to find a link between the two different methods used by Ebert and Kestenband. For this reason, we start by describing the two methods.

Kestenband [12] considers a $(2n+1)\times(2n+1)$ Hermitian matrix H over $\mathbb{F}_{q^2}$ with a primitive characteristic polynomial, defined over $\mathbb{F}_q$. He then considers the set of Hermitian varieties $\chi = \{\bar{x}^{\mathrm{t}} H^i \bar{x}^{(q)} = 0 \| i=0,\dots,(q^{2n+1}-q)/(q-1),\ \bar{x} \in \mathrm{PG}(2n,q^2)\}$ and proves:

Theorem 15. *Any* $2n$ *linearly independent Hermitian varieties of* χ *intersect in a* $(q^{2n+1}+1)/(q+1)$*-cap of* $\mathrm{PG}(2n,q^2)$ *and any two such distinct caps are disjoint.*

To construct the caps, Ebert represents $\mathrm{PG}(2n,q^2)$ by $\mathbb{F}_{q^{4n+2}} \pmod{\mathbb{F}_{q^2}}$. So the points of $\mathrm{PG}(2n,q^2)$ are the non-zero elements of $\mathbb{F}_{q^{4n+2}}$ and two elements x and y of $\mathbb{F}_{q^{4n+2}}$ define the same point of $\mathrm{PG}(2n,q^2)$ if and only if $x/y \in \mathbb{F}_{q^2}$. The point of $\mathrm{PG}(2n,q^2)$ represented by $x \in \mathbb{F}^*_{q^{4n+2}}$ is denoted by (x).

By Theorem 3, the hyperplanes of $\mathrm{PG}(2n,q^2)$ are the sets $[u]=\{(x) \in \mathbb{F}_{q^{4n+2}} \pmod{\mathbb{F}_{q^2}} \| \mathrm{Tr}_{\mathbb{F}_{q^{4n+2}}/\mathbb{F}_{q^2}}(ux)=0\}$, for $u \in \mathbb{F}^*_{q^{4n+2}}$, where $[u]=[w]$, $u,w \in \mathbb{F}^*_{q^{4n+2}}$, if and only if $u/w \in \mathbb{F}_{q^2}$.

A mapping $\alpha : (x) \mapsto (\beta x)$, with β a primitive element of $\mathbb{F}_{q^{4n+2}}$, is a Singer cycle of $\mathrm{PG}(2n,q^2)$, that is, a projective transformation acting in one orbit on $\mathrm{PG}(2n,q^2)$.

Using this description, Ebert [4] proves

Theorem 16. *The orbits of size* $M=(q^{2n+1}+1)/(q+1)$*, under* $\langle \xi \rangle$*, where* $\xi=\alpha^N$ *with* $N=(q^{2n+1}-1)/(q-1)$*, are* M*-caps of* $\mathrm{PG}(2n,q^2)$.

4.2. Equivalence of the two constructions

First of all, the next theorem shows that the caps by Ebert are of the type discussed by Kestenband.

Theorem 17 (Cossidente and Storme [2]). *A* M*-cap fixed by* $\langle \xi \rangle$ *is the intersection of* $2n$ *linearly independent Hermitian varieties*

$$H_a = \{(x) \in \mathrm{PG}(2n,q^2) \| \mathrm{Tr}_{\mathbb{F}_{q^{4n+2}}/\mathbb{F}_{q^2}}(ax^{q^{2n+1}+1}) = 0\},$$

with $a \in \mathbb{F}_{q^{4n+2}}$, $a^{q^{2n+1}-1} \in \mathbb{F}_{q^2}$.

By now using a self-dual normal basis, it will be shown that the caps by Kestenband are of the type described by Ebert. The method we apply extends the one by Boros and Szönyi [1, pp. 265–268] to arbitrary spaces $\mathrm{PG}(2n,q^2)$.

First of all, construct a self-dual normal basis B of $\mathbb{F}_{q^{4n+2}}$ over $\mathbb{F}_{q^2}$ [11, Theorem 5.2.1; 13]. This means that $B=\{d, d^{q^2}, \ldots, d^{q^{4n}}\}$ for some $d \in \mathbb{F}_{q^{4n+2}}$ with $\mathrm{Tr}_{\mathbb{F}_{q^{4n+2}}/\mathbb{F}_{q^2}}(d^{q^{2i}} d^{q^{2j}}) = \delta_{ij}$ for $i,j=0,\ldots,2n$.

Construct now the matrix $E=(e_{ij})$, $0 \leqslant i, j \leqslant 2n$, with $e_{ij}=d^{q^{2i+2j}}$. Then $E^2=I_{2n+1}$ where I_{2n+1} is the identity matrix of rank $2n+1$.

Consider the isomorphism

$$\phi : (\mathbb{F}_{q^2})^{2n+1} \to P = \{(x, x^{q^2}, \ldots, x^{q^{4n}}) \| x \in \mathbb{F}_{q^{4n+2}}\} \quad \text{via } \bar{x} \mapsto (E\bar{x}^{\mathrm{t}})^{\mathrm{t}},$$

where $\bar{x}=(x_0,\ldots,x_{2n})$, which implies an isomorphism between $\mathrm{PG}(2n,q^2)$ and $\bar{P}=\{(x, x^{q^2}, \ldots, x^{q^{4n}}) \| x \in \mathbb{F}_{q^{4n+2}} \pmod{\mathbb{F}_{q^2}}\}$.

By Jamison [10, pp. 258–259], every linear mapping f of $\mathbb{F}_{q^{4n+2}}$ is of type $f : \mathbb{F}_{q^{4n+2}} \to \mathbb{F}_{q^{4n+2}} : x \mapsto a_0 x + a_1 x^{q^2} + \cdots + a_{2n} x^{q^{2(2n)}}$, for some $a_i \in \mathbb{F}_{q^{4n+2}}$, $i=0,\ldots,2n$.

So, since the points of P have coordinates $(x, x^{q^2}, \ldots, x^{q^{4n}})$, a linear mapping on P is of type

$$\begin{pmatrix} x \\ x^{q^2} \\ \vdots \\ x^{q^{4n}} \end{pmatrix} \mapsto \begin{pmatrix} a_0 & a_1 & \cdots & a_{2n} \\ a_{2n}^{q^2} & a_0^{q^2} & \cdots & a_{2n-1}^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{4n}} & a_2^{q^{4n}} & \cdots & a_0^{q^{4n}} \end{pmatrix} \begin{pmatrix} x \\ x^{q^2} \\ \vdots \\ x^{q^{4n}} \end{pmatrix}.$$

The isomorphism ϕ can be extended in a natural way to the linear transformations. Namely, for each linear transformation T of $(\mathbb{F}_{q^2})^{2n+1}$, let $\phi(T) = ETE^{-1} = ETE$ be the corresponding linear transformation of P.

Denoting the matrix of the above mentioned mapping on P by $[a_0, \ldots, a_{2n}]$, ϕ has the following properties which are of particular interest to us [1, p. 267].

Lemma 18. (1) *The two matrices $\phi(T)$ and T have the same characteristic polynomial.*

(2) *If $d \in \mathbb{F}_{q^{2n+1}}$, then T is a Hermitian matrix of $\mathrm{GL}(2n+1, q^2)$ if and only if $\phi(T) = [a_0, \ldots, a_{2n}]$ is a Hermitian matrix of $\mathrm{GL}(2n+1, q^{4n+2})$.*

Lemma 19. *A self-dual normal basis of $\mathbb{F}_{q^{2n+1}}$ over $\mathbb{F}_q$ defines a self-dual normal basis of $\mathbb{F}_{q^{4n+2}}$ over $\mathbb{F}_{q^2}$.*

Proof. As $\gcd(2n+1, 2) = 1$, for $x \in \mathbb{F}_{q^{2n+1}}$, necessarily $\mathrm{Tr}_{\mathbb{F}_{q^{2n+1}}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_{q^{4n+2}}/\mathbb{F}_{q^2}}(x)$. □

Theorem 20. *The constructions of the $(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n, q^2)$ by Ebert and Kestenband are equivalent.*

Proof. The proof follows the reasoning of [1, pp. 265–268].

Consider first of all a self-dual normal basis $B = \{d, d^{q^2}, \ldots, d^{q^{4n}}\}$ of $\mathbb{F}_{q^{4n+2}}$ over $\mathbb{F}_{q^2}$ with $d \in \mathbb{F}_{q^{2n+1}}$ (Lemma 19). Let ϕ be the mapping, defined in this section, corresponding to B.

Consider the Hermitian variety $H = \{\bar{x} \in \mathrm{PG}(2n, q^2) \| \bar{x}^{\mathrm{t}} H \bar{x}^{(q)} = 0\}$ where H has a primitive characteristic polynomial, defined over $\mathbb{F}_q$. Applying ϕ on H gives a Hermitian matrix $\phi(H) = [a_0, \ldots, a_{2n}]$ (Lemma 18(2)).

Since H and $\phi(H)$ have the same irreducible characteristic polynomial (Lemma 18), all characteristic roots of $\phi(H)$ are conjugate elements $\lambda, \lambda^q, \ldots, \lambda^{q^{2n}}$ of $\mathbb{F}_{q^{2n+1}}$ over $\mathbb{F}_q$. If $(x_0, \ldots, x_{2n}) \in \mathbb{F}_{q^{4n+2}}^{2n+1}$ is a right-eigenvector of $\phi(H)$ corresponding to the eigenvalue λ, then $(x_{2n}^{q^2}, x_0^{q^2}, \ldots, x_{2n-1}^{q^2}), \ldots, (x_1^{q^{4n}}, \ldots, x_{2n}^{q^{4n}}, x_0^{q^{4n}})$ are right-eigenvectors of $\phi(H)$ corresponding to the eigenvalues $\lambda^{q^2}, \ldots, \lambda^{q^{4n}}$.

Let $W = [x_0^{q^{2n+1}}, \ldots, x_{2n}^{q^{2n+1}}]^{\mathrm{t}}$. A reasoning similar to [1, p. 268] shows, with $W^* = \bar{W}^{\mathrm{t}}$ where $\bar{W}$ is the conjugate of W over $\mathbb{F}_{q^{2n+1}}$, that $W^* W = [\mu, 0, \ldots, 0]$ for some $\mu \in \mathbb{F}_{q^{2n+1}}$. Since $\mu \in \mathbb{F}_{q^{2n+1}}$, $\mu = (1/\xi)^{q^{2n+1}+1}$ for some $\xi \in \mathbb{F}_{q^{4n+2}}$. Replacing $(x_0, \ldots, x_{2n})$ by

Table 1
Generator polynomials

(1)	$(q^{2n+1}+1)/(q+1)$-caps in $\mathrm{PG}(2n,q^2)$	$g(X)$ the minimal polynomial of degree $2n+1$ over $\mathbb{F}_{q^2}$ of a primitive $(q^{2n+1}+1)(q-1)$-th root of unity.
(2)	(q^n-1)-caps in $\mathrm{PG}(2n,q)$	$g(X)=(X-1)h(X)h(1/X)X^n$ where h is a primitive polynomial of degree n over $\mathbb{F}_q$.
(3)	(q^n+1)-caps in $\mathrm{PG}(2n-1,q)$, n even	$g(X)$ the minimal polynomial of degree $2n$ over $\mathbb{F}_q$ of a primitive $(q^n+1)(q-1)$-th root ξ of unity.
(4)	(q^n+1)-caps in $\mathrm{PG}(2n,q)$	$g(X)=(X-1)g(X)$ with $g(X)$ the minimal polynomial of degree $2n$ over $\mathbb{F}_q$, of a primitive (q^n+1)-th root of unity.
(5)	$(q^n+1)(q-1)$-caps in $\mathrm{PG}(2n+1,q)$	$g(X)=(X-1)(X-\eta)g_1(X)$ with $g_1(X)$ as in (3) and with $\eta=\xi^{q^n+1}$.
(6)	$(q^n+1)(q+1)$-caps in $\mathrm{PG}(2n+1,q)$, n even	$g(X)=g_1(X)g_2(X)$ with g_1 and g_2 the minimal polynomials of degree $2n$ and two, over $\mathbb{F}_q$, of β and η (Theorem 14).
(7)	$\frac{(q^n-1)(q+1)}{\gcd(q-1,2)}$-caps in $\mathrm{PG}(2n+1,q)$, n odd	$g(X)=h(X)X^nh(1/X)g_2(X)$ with h as in (2) and with g_2 the minimal polynomial of degree two, over $\mathbb{F}_q$, of a primitive $(q+1)$-th root of unity.

$(\xi x_0,\ldots,\xi x_{2n})$ and proceeding as before, gives a new matrix W satisfying $W^*W=I_{2n+1}$.

Since $\phi(H)=EHE^{-1}$ implies $\phi(H^r)=(\phi(H))^r$, we have $W^{\mathrm{t}}(\phi(H^r))W^{(q^{2n+1})}=[\lambda^r,0,\ldots,0]$. So changing the reference system such that $\bar{x}=W\bar{y}$, with $\bar{y}$ the new coordinate, the Hermitian variety $\bar{x}^{\mathrm{t}}\phi(H^r)\bar{x}^{(q^{2n+1})}=0$ is mapped onto $\bar{y}^{\mathrm{t}}[\lambda^r,0,\ldots,0]\bar{y}^{(q^{2n+1})}=0$. Hence, a point $(x,x^{q^2},\ldots,x^{q^{4n}})$ belongs to this Hermitian variety if and only if

$$(x,x^{q^2},\ldots,x^{q^{4n}})[\lambda^r,0,\ldots,0](x^{q^{2n+1}},x^{q^{2n+3}},\ldots,x^{q^{4n+2n+1}})^{\mathrm{t}}=\mathrm{Tr}_{\mathbb{F}_{q^{4n+2}}/\mathbb{F}_{q^2}}(\lambda^r x^{q^{2n+1}+1})=0. \quad (1)$$

Since ϕ maps linearly independent Hermitian varieties of χ with matrices $H^{i_1},\ldots,H^{i_{2n}}$ onto linearly independent Hermitian varieties $H_{\lambda^{i_1}},\ldots,H_{\lambda^{i_{2n}}}$ (Theorem 17), ϕ is an isomorphism between their intersections which is in the first case a cap by Kestenband (Theorem 15) and in the second case a cap by Ebert (Theorem 17). □

5. Conclusion

Table 1 summarizes the list of known infinite classes of cyclic caps. For each class, also the generator polynomial of the corresponding pseudo-cyclic code is presented. We recall that the minimal polynomial over $\mathbb{F}_q$ of an element β of $\mathbb{F}_{q^n}$ is the smallest degree monic polynomial $g(X)\in\mathbb{F}_q[X]$ for which $g(\beta)=0$.

In Case (3), the generator polynomial for the pseudo-cyclic code C corresponding with the cyclic (q^n+1)-cap in $\mathrm{PG}(2n-1,q)$, n even, is the minimal polynomial of degree $2n$ over $\mathbb{F}_q$ of a primitive $(q^n+1)(q-1)$-th root ξ of unity because in Theorem 4, such a cap is generated by $\langle\xi\rangle$ where ξ is the $N=(q^n-1)/(q-1)$-th power of a cyclic Singer group $\langle\beta\rangle$. Hence $\langle\beta\rangle$ defines a pseudo-cyclic code with a primitive polynomial of degree $2n$ over $\mathbb{F}_q$ as generator polynomial and so the generator polynomial of C is the minimal polynomial of a primitive $(q^{2n}-1)/N=(q^n+1)(q-1)$-th root of unity.

In Case (5), the generator polynomial is $g(X)=(X-1)(X-\eta)g_1(X)$ since in this case the caps are orbits under the group generated by $\alpha:(x,y,z)\mapsto(\xi x,\eta y,z)$ (Theorem 10). Hence $\alpha(0,0,1)=(0,0,1)$ and this defines the factor $X-1$, $\alpha(0,1,0)=(0,\eta,0)$ which defines the factor $X-\eta$, and $\alpha(x,0,0)=(\xi x,0,0)$, with ξ as above, and this defines the factor $g_1(X)$, with $g_1(X)$ defined in (3).

The other generator polynomials are obtained in the same way.

Remark 21. The preceding results show that it is possible to construct cyclic caps which are the intersection of quadrics in $\mathrm{PG}(n,q)$ or of Hermitian varieties in $\mathrm{PG}(2n,q^2)$.

Hence, only the question remains whether there exist cyclic caps which are the intersection of Hermitian varieties in odd-dimensional projective spaces.

We will now use elementary abelian groups to construct caps on quadrics.

6. Elementary abelian caps on quadrics

6.1. Elementary abelian q^{2n}-caps in $\mathrm{PG}(3n,q)$

Consider $\mathrm{PG}(3n,q)\cong\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_q\,(\mathrm{mod}\,\mathbb{F}_q)$ so that a point is $\rho(x_0,x_1,x_2,x_3)$, $\rho\in\mathbb{F}_q^*$, $(x_0,x_1,x_2,x_3)\in(\mathbb{F}_{q^n}^3\times\mathbb{F}_q)^*$ and a hyperplane is $[u,v,w,t]=\{(x_0,x_1,x_2,x_3)\|\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ux_0+vx_1+wx_2)+tx_3=0\}$, with $u,v,w\in\mathbb{F}_{q^n}$, $t\in\mathbb{F}_q$, $(u,v,w,t)\neq(0,0,0,0)$.

Lemma 22. *Fix $a,b\in\mathbb{F}_{q^n}$ so that $X_0^2+aX_0X_1+bX_1^2$ is an irreducible polynomial over $\mathbb{F}_{q^n}$.*

Then the set $Q_{\alpha,\beta}=\{(x_0,x_1,x_2,x_3)\in(\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_{q^n}\times\mathbb{F}_q)\,(\mathrm{mod}\,\mathbb{F}_q)\|\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha(X_0^2+aX_0X_1+bX_1^2-X_2X_3))+\beta X_3^2=0\}$, with $\alpha\in\mathbb{F}_{q^n},\beta\in\mathbb{F}_q,(\alpha,\beta)\neq(0,0)$, is:

(i) *a singular quadric with as vertex a $(n-2)$-dimensional subspace and with base a non-singular elliptic quadric $E_{2n+1,q}$ in a $(2n+1)$-dimensional subspace $\mathrm{PG}(2n+1,q)$ skew to the vertex when $\alpha\neq0$;*

(ii) *the hyperplane $X_3=0$, counted with multiplicity two, when $\alpha=0$.*

Proof. To prove this, the arguments of [3] can be used. Since these quadrics are singular, we briefly sketch the proof to make clear the singular space.

We use the characterization result [9, Theorem 22.10.23].

Let $(x_0,\ldots,x_3)\in Q_{\alpha,\beta},\alpha\neq0$. A line $(x_0+\lambda y_0,\ldots,x_3+\lambda y_3)$ intersects $Q_{\alpha,\beta}$ in the points satisfying $\mathrm{Tr}(\alpha(x_0^2+ax_0x_1+bx_1^2-x_2x_3))+\beta x_3^2+\lambda[\mathrm{Tr}(2\alpha x_0y_0+\alpha a(x_0y_1+$

$x_1y_0) + \alpha b2x_1y_1 - \alpha(x_2y_3 + x_3y_2)) + 2\beta x_3y_3] + \lambda^2(\mathrm{Tr}(\alpha(y_0^2 + ay_0y_1 + by_1^2 - y_2y_3)) + \beta y_3^2) = 0$.

Hence this line is a tangent line if and only if the coefficient of λ is zero, and this is equivalent to $(y_0,\dots,y_3) \in [2\alpha x_0 + \alpha a x_1, \alpha a x_0 + 2\alpha b x_1, -\alpha x_3, \mathrm{Tr}(-\alpha x_2) + 2\beta x_3]$. The latter set is a hyperplane unless $2\alpha x_0 + \alpha a x_1 = 0, \alpha a x_0 + 2\alpha b x_1 = 0, x_3 = 0, \mathrm{Tr}(-\alpha x_2) + 2\beta x_3 = 0$, and this is equivalent to $x_0 = x_1 = x_3 = 0, \mathrm{Tr}(-\alpha x_2) = 0$ since $X^2 + aX + b$ is irreducible over $\mathbb{F}_{q^n}$.

A point $(0,0,x_2,0)$ with $\mathrm{Tr}(-\alpha x_2) = 0$ belongs to $Q_{\alpha,\beta}$. Hence $Q_{\alpha,\beta}$ has a singular space of dimension $n-2$. To prove that the base is a non-singular elliptic quadric, consider $\{(x_0,x_1,x_2'x_2'',x_3) \| x_0,x_1 \in \mathbb{F}_{q^n}, x_2'' \in \mathbb{F}_{q^n}$ fixed with $\mathrm{Tr}(\alpha x_2'') \neq 0, x_2', x_3 \in \mathbb{F}_q\}$. This intersects $Q_{\alpha,\beta}$ in the set of points satisfying $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha(X_0^2 + aX_0X_1 + bX_1^2)) - \mathrm{Tr}(\alpha x_2'')X_2'X_3 + \beta X_3^2 = 0$ which is a non-singular elliptic quadric in this $(2n+1)$-dimensional space [3, Lemma 4.3]. □

Theorem 23. *The intersection of n linearly independent quadrics $Q_{\alpha_1,\beta_1},\dots,Q_{\alpha_n,\beta_n}$, with $Q_{0,1}$ not linearly dependent on $Q_{\alpha_1,\beta_1},\dots,Q_{\alpha_n,\beta_n}$, is the disjoint union of an elementary abelian q^{2n}-cap and the subspace $X_0 = X_1 = X_3 = 0$.*

Proof. The quadrics $Q_{\alpha,\beta}$ are fixed by the elementary abelian group G of elements $(x_0,x_1,x_2,x_3) \mapsto (x_0 + l_1x_3, x_1 + l_2x_3, (2l_1 + al_2)x_0 + (al_1 + 2bl_2)x_1 + x_2 + (l_1^2 + al_1l_2 + bl_2^2)x_3, x_3), l_1, l_2 \in \mathbb{F}_{q^n}$.

Using the arguments of [3,12], it is possible to prove that j linearly independent quadrics $Q_{\alpha_1,\beta_1},\dots,Q_{\alpha_j,\beta_j}$, with $Q_{0,1}$ not linearly dependent on these quadrics, intersect in $(q^{3n+1-j} + q^{2n-j} - q^{2n} - 1)/(q-1)$ points. Hence $|\bigcap_{i=1}^n Q_{\alpha_i,\beta_i}| = q^{2n} + (q^n - 1)/(q-1)$.

This intersection consists of the $(n-1)$-dimensional subspace $X_0 = X_1 = X_3 = 0$ and q^{2n} other points.

For such a point (x_0,x_1,x_2,x_3), we have $x_3 \neq 0$. Namely, if we assume $x_3 = 0$, then this point satisfies $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i(x_0^2 + ax_0x_1 + bx_1^2)) = 0$, $i = 1,\dots,n$. The elements $\alpha_1,\dots,\alpha_n$ form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ since $Q_{0,1}$ is not linearly dependent on Q_{α_i,β_i}, $i = 1,\dots,n$.

Hence $x_0^2 + ax_0x_1 + bx_1^2 = 0$ and so $x_0 = x_1 = 0$ since $X_0^2 + aX_0X_1 + bX_1^2$ is irreducible over $\mathbb{F}_{q^n}$. So we do not have one of the remaining q^{2n} points.

One then shows the q^{2n} other points form an orbit under G, of size q^{2n}, of a point $(x_0,x_1,x_2,1)$. This latter orbit is a q^{2n}-cap. □

6.2. A cap in $\mathrm{PG}(3n+1,q)$

We now generalize [17, Proposition II]. Let $\mathrm{PG}(3n+1,q) \cong \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q \times \mathbb{F}_q \pmod{\mathbb{F}_q}$ so that a point is $\rho(x_0,\dots,x_4)$ with $\rho \in \mathbb{F}_q^*, x_3,x_4 \in \mathbb{F}_q$, $x_0,x_1,x_2 \in \mathbb{F}_{q^n}$, $(x_0,\dots,x_4) \neq (0,\dots,0)$ and a hyperplane is $[u,v,w,t,s] = \{(x_0,\dots,x_4) \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ux_0 + vx_1 + wx_2) + tx_3 + sx_4 = 0\}$, with $u,v,w \in \mathbb{F}_{q^n}$, $t,s \in \mathbb{F}_q$, $(u,v,w,t,s) \neq (0,\dots,0)$.

Lemma 24. *Fix $a,b \in \mathbb{F}_{q^n}$ so that $X_0^2 + aX_0X_1 + bX_1^2$ is an irreducible polynomial over $\mathbb{F}_{q^n}$.*

Then the set $Q_{\alpha,\beta,\gamma,\delta} = \{(x_0,x_1,x_2,x_3,x_4) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q \times \mathbb{F}_q)(\mathrm{mod}\, \mathbb{F}_q) \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha(X_0^2 + aX_0X_1 + bX_1^2 - X_2X_3)) + \beta X_3^2 + \gamma X_3X_4 + \delta X_4^2 = 0\}$, *with* $\beta,\gamma,\delta \in \mathbb{F}_q$, $(\beta,\gamma,\delta) \neq (0,0,0)$, *is*:

(i) *a singular quadric with a* $(n-1)$*-dimensional vertex and a non-singular elliptic quadric* $E_{2n+1,q}$ *in a* $(2n+1)$*-dimensional subspace skew to the vertex as base when* $\delta = 0$ *and* $\alpha \neq 0$;

(ii) *a singular quadric with a* $(n-2)$*-dimensional vertex and a non-singular parabolic quadric* $P_{2n+2,q}$ *in a* $(2n+2)$*-dimensional subspace skew to the vertex as base when* $\delta \neq 0$ *and* $\alpha \neq 0$;

(iii) *the union of two distinct hyperplanes, one hyperplane with multiplicity two, or the subspace* $X_3 = X_4 = 0$ *when* $\alpha = 0$ *and* $\beta X_3^2 + \gamma X_3X_4 + \delta X_4^2$ *is respectively the union of two distinct factors over* $\mathbb{F}_q$*, a square, or irreducible over* $\mathbb{F}_q$.

Proof. This is proved by using an argument similar to the proof of Lemma 22. □

We now consider a $(n+1)$-dimensional vector space V of quadrics generated by quadrics $Q_{\alpha_i,\beta_i,\gamma_i,\delta_i}$, $i = 1,\ldots,n+1$, satisfying the following conditions:

(a) $\{\alpha_1,\ldots,\alpha_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$;

(b) V contains a quadric $Q_{0,\beta,\gamma,\delta}$ which is the union of two distinct hyperplanes, with $\delta \neq 0$.

Theorem 25. *The quadrics of* V *intersect in the subspace* $X_0 = X_1 = X_3 = X_4 = 0$ *and in a* $2q^{2n}$*-cap.*

Proof. This cap consists of two disjoint q^{2n}-caps of Theorem 23 in the two hyperplanes defined by the linear factors of $Q_{0,\beta,\gamma,\delta}$. □

6.3. *An elementary abelian* q^{2n+1}*-cap in* $\mathrm{PG}(3n+2,q)$

Let $\mathrm{PG}(3n+2,q) \cong \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q (\mathrm{mod}\, \mathbb{F}_q)$ so that the points are $\rho(x_0,\ldots,x_5)$, $\rho \in \mathbb{F}_q^*$, $x_0,x_1,x_2 \in \mathbb{F}_{q^n}$, $x_3,x_4,x_5 \in \mathbb{F}_q$, $(x_0,\ldots,x_5) \neq (0,\ldots,0)$ and the hyperplanes are $[u_0,\ldots,u_5] = \{(x_0,\ldots,x_5) \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(u_0x_0 + \cdots + u_2x_2) + u_3x_3 + \cdots + u_5x_5 = 0\}$ with $u_0,u_1,u_2 \in \mathbb{F}_{q^n}$, $u_3,u_4,u_5 \in \mathbb{F}_q$, $(u_0,\ldots,u_5) \neq (0,\ldots,0)$.

Fix $a,b \in \mathbb{F}_{q^n}$ so that $X_0^2 + aX_0X_1 + bX_1^2$ is an irreducible polynomial over $\mathbb{F}_{q^n}$.

Consider the set of quadrics $Q_{\alpha,\beta,\gamma} = \{(x_0,\ldots,x_5) \in (\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \times \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q)(\mathrm{mod}\, \mathbb{F}_q) \| \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha(X_0^2 + aX_0X_1 + bX_1^2 - X_2X_3)) + \beta X_3^2 + \gamma(X_4^2 - X_3X_5) = 0\}$, with $\alpha \in \mathbb{F}_{q^n}, \beta,\gamma \in \mathbb{F}_q$, $(\alpha,\beta,\gamma) \neq (0,0,0)$.

Lemma 26. *For* $\alpha \neq 0$, $Q_{\alpha,\beta,\gamma}$ *is*:

(i) *a singular quadric with a* $(n-1)$*-dimensional vertex and with base a non-singular quadric* $P_{2n+2,q}$ *in a* $(2n+2)$*-dimensional subspace skew to the vertex when* $\gamma \neq 0$;

(ii) *a singular quadric with a n-dimensional vertex and with base a non-singular elliptic quadric* $E_{2n+1,q}$ *in a* $(2n+1)$*-dimensional subspace skew to the vertex when* $\gamma = 0$.

For $\alpha = 0$, $Q_{0,\beta,0}$ *is the hyperplane* $X_3 = 0$ *counted with multiplicity two and* $Q_{0,\beta,\gamma}$, $\gamma \neq 0$, *is a cone with vertex* $X_3 = X_4 = X_5 = 0$, *and with base the conic* $\beta X_3^2 + \gamma(X_4^2 - X_3X_5) = 0$ *in* $X_0 = X_1 = X_2 = 0$.

Proof. This again is proved by using the arguments of the proof of Lemma 22. □

Theorem 27. *Let* V *be a* $(n+1)$*-dimensional vector space of quadrics, with* $Q_{0,1,0} \notin V$. *Then the quadrics of* V *intersect in the subspace* $X_0 = X_1 = X_3 = X_4 = 0$ *and in an elementary abelian* q^{2n+1}*-cap.*

Proof. Here the arguments of the previous results can be copied. The intersection of j linearly independent quadrics $Q_{\alpha_i,\beta_i,\gamma_i}$, where $\alpha_1 = 0$, $\alpha_2, \ldots, \alpha_j$ are linearly independent over $\mathbb{F}_q$, not all γ_i are zero, and where $Q_{0,1,0}$ is not linearly dependent on these quadrics, contains $(q^{3n+3-j} - q^{2n+1} + q^{2n+2-j} - 1)/(q-1)$ points. So for $j = n+1$, the intersection contains $q^{2n+1} + (q^{n+1} - 1)/(q-1)$ points.

The cap is an orbit of a point $(x_0, x_1, x_2, 1, x_4, x_5)$ under the elementary abelian group of transformations $(x_0, \ldots, x_5) \mapsto (x_0 + l_1x_3, x_1 + l_2x_3, (2l_1 + al_2)x_0 + (al_1 + 2bl_2)x_1 + x_2 + (l_1^2 + al_1l_2 + bl_2^2)x_3, x_3, t_2x_3 + x_4, t_2^2x_3 + 2t_2x_4 + x_5)$, with $l_1, l_2 \in \mathbb{F}_{q^n}, t_2 \in \mathbb{F}_q$, which fixes all quadrics $Q_{\alpha,\beta,\gamma}$. □

References

[1] E. Boros, T. Szőnyi, On the sharpness of a theorem of B. Segre, Combinatorica 6 (1986) 261–268.

[2] A. Cossidente, L. Storme, Caps on elliptic quadrics, Finite Fields Appl. 1 (1995) 412–420.

[3] A. Cossidente, L. Storme, Caps on parabolic and hyperbolic quadrics, in: Recent Progress in Geometry (special issue), Rend. Circ. Mat. Palermo 51 (II) (1998) 57–69.

[4] G.L. Ebert, Partitioning projective geometries into caps, Canad. J. Math. XXXVII (6) (1985) 1163–1175.

[5] Y. Edel, J. Bierbrauer, 41 is the largest size of a cap in PG(4,4), Des. Codes Cryptogr., to appear.

[6] D.G. Glynn, On a set of lines of PG$(3,q)$ corresponding to a maximal cap contained in the Klein quadric in PG$(5,q)$, Geom. Dedicata 26 (1988) 273–280.

[7] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, Oxford, 1979.

[8] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Oxford University Press, Oxford, 1985.

[9] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Oxford University Press, Oxford, 1991.

[10] R.E. Jamison, Covering finite fields with cosets of subspaces, J. Combin. Theory, Ser. A 22 (1977) 253–266.

[11] D. Jungnickel, Finite Fields: Structure and Arithmetics, Bibliographisches Institut, Mannheim, 1993.

[12] B.C. Kestenband, Projective geometries that are disjoint unions of caps, Canad. J. Math. XXXII (6) (1980) 1299–1305.

[13] A. Lempel, M.J. Weinberger, Self-complementary normal bases in finite fields, SIAM J. Discrete Math. 1 (1988) 193–198.

[14] T. Maruta, A geometric approach to semi-cyclic codes, in: J.W.P. Hirschfeld, D.R. Hughes, J.A. Thas (Eds.), Advances in Finite Geometries and Designs, Oxford University Press, Oxford, 1991, pp. 311–318.

[15] G. Seroussi, A. Lempel, Factorization of symmetric matrices and trace-orthogonal bases in finite fields, SIAM J. Comput. 9 (4) (1980) 758–767.
[16] J. Singer, A theorem in finite projective geometry and some applications to number theory, Trans. Amer. Math. Soc. 43 (1938) 377–385.
[17] G. Tallini, Calotte complete di $S_{4,q}$ contenenti due quadriche ellittiche quali sezioni iperpiane, Rend. Mat. Appl. 23 (1964) 108–123.